

24 June 2025

FOI Ref 21393

Request - You asked us the following:

1. The number of data breach incidents the force has had in the last three years (Broken down by financial years 2022/23, 2023/24 and 2024/25)

1a) Of those, how many were cyber incidents? (Broken down by years as above)

1b) Can these be broken down by year and by incident type? E.g. instances where data was emailed to the incorrect recipient or cases of loss/theft of devices containing personal data etc.? (Broken down by years as above)

2. How many compensation claims have been brought against the force for data breaches in the last three years (Broken down by financial years 2022/23, 2023/24 and 2024/25)

2a) Of those, how many were settled with compensation and how many were refused?

2b) How much has the force paid out in compensation for data breach claims in the last three years? (Broken down by years as above)

If possible, can this be presented in PDF format please?

Clarification received on 28/05/2025

Yes, could you please provide the amount paid by the force in relation to the compensation claims in question 2.

We received your request on 27/05/2025 and have processed this under the Freedom of Information Act (FOIA).

Staffordshire Police's response to your enquiry is as follows:

Staffordshire Police holds some of the requested information.

- 1. The number of data breach incidents the force has had in the last three years (Broken down by financial years 2022/23, 2023/24 and 2024/25) – **Partially disclosed, please see the below exemptions.**
2022/2023 – 227
2023/2024 – 539
2024/2025 – 405
- 1a) Of those, how many were cyber incidents? (Broken down by years as above) – **Neither confirm nor deny, please see the below exemptions.**
- 1b) Can these be broken down by year and by incident type? E.g. instances where data was emailed to the incorrect recipient or cases of loss/theft of devices containing personal data etc.? (Broken down by years as above) – **Partially disclosed, please see the accompanying file titled 'FOI 21393 Data Breaches Data'. Please see the below exemptions.**



- 2. How many compensation claims have been brought against the force for data breaches in the last three years (Broken down by financial years 2022/23, 2023/24 and 2024/25) – **Partially disclosed, please see the below exemptions.**
2022/2023 – 4
2023/2024 – 6
2024/2025 – 5
- 2a) Of those, how many were settled with compensation and how many were refused?
– **Partially disclosed, please see the below exemptions.**
2022/2023 – 3 settled, 1 refused and 4 ongoing
2023/2024 – 1 settled, nil refused and 5 ongoing
2024/2025 – nil settled, nil refused and 5 ongoing
- 2b) How much has the force paid out in compensation for data breach claims in the last three years? (Broken down by years as above) – **Partially disclosed, please see the below exemptions.**
2022/2023 - £27,000
2023/2024 - £1,500
2024/2025 – not applicable
Please note that the above costs are for compensation paid only and do not include solicitors costs.

Please be advised that the data for question 2, 2a and 2b all relate to the same claims.

Please note that this data has been provided to the best of our ability, subject to the limitation of current recording protocols and systems/software. Additional incidents may have been recorded during these timescales but are awaiting finalisation and input onto these systems and would not be present within this dataset.

Every effort is made to ensure that the data presented is accurate and complete. However, it is important to note that this has been extracted from multiple sources, developed for specific policing purposes, for which data extraction methods have not been specifically designed to directly correlate with the terminology of this request. Therefore, the data presented is subject to the inaccuracies and idiosyncrasies inherent in any large-scale recording system.

As a consequence, care should be taken in the interpretation and presentation of this data, so as to not misrepresent the whole or any part of the data disclosed.

Please be advised that all Freedom of Information request responses are published on the Staffordshire Police website although personal details are not included.

Staffordshire Police can neither confirm nor deny whether any further information relevant to this request is held, as the duty in Section 1(1)(a) of the Freedom of Information Act 2000 does not apply by virtue of the following exemptions:

In accordance with Section 17(1) of the Freedom of Information Act, this letter represents a refusal notice for this particular request.

- Section 24(2) National Security
- Section 31(3) Law Enforcement

Section 24 and Section 31 are both qualified exemptions and as such there is a requirement to evidence any harm confirmation or denial that any other information is held as well as consider the public interest.

Harm in Confirming or Denying that Information is held

To confirm or deny whether any further information is held in respect of successful cyber attacks resulting in Data Breaches would provide actual knowledge that where an attempt has been made, it has or has not been successful. Confirming that such information is not held may assist potential attackers by indicating that an attack had gone undetected. Equally, confirming information is held would enable understanding of where attacks have been successful, and possible weaknesses exist. Attackers may then be able to tailor their methods to increase their chances of success.

To confirm or deny whether information is held in respect of any leaked data as a result of an attack would, in effect, confirm that there had been successful cyber attacks made against the force, which would present harm as detailed above.

Furthermore, in order to counter criminal and terrorist behaviour it is vital that the police and other agencies have the ability to work together, where necessary covertly, in order to obtain intelligence within current legislative frameworks to ensure the arrest and prosecution of offenders who commit or plan to commit acts of terrorism, whereby their modus operandi may involve cyber attacks on secure databases. In order to achieve this goal, it is vitally important that information sharing takes place with other police forces and security bodies within the United Kingdom in order to support counter-terrorism measures in the fight to deprive terrorist networks of their ability to commit crime. To confirm or deny specific details of any breaches of information technology and security would be extremely useful to those involved in terrorist activity as it would enable them to map vulnerable information security databases.

Public Interest Test

Section 24(2) National Security

Factors in favour of confirming or denying that information is held

The public are entitled to know how public funds are spent and how resources are distributed within an area of policing. To confirm information is held regarding successful cyber-attacks causing Data Breaches would enable the general public to hold Staffordshire Police to account ensuring all such breaches are recorded and investigated appropriately. With the call for transparency of public spending this would enable improved public debate.

Factors against confirming or denying that information is held

Security measures are put in place to protect the community we serve. As evidenced within the harm to confirm whether any cyber-attacks have been successful would highlight to terrorists and individuals intent on carrying out criminal activity vulnerabilities within Staffordshire Police which could be further exploited.

Taking into account the current security climate within the United Kingdom, no information (such as the citing of an exemption which confirms information pertinent to this request is held, or conversely, stating 'no information is held') which may aid a terrorist should be disclosed. To what extent this information may

aid a terrorist is unknown, but it is clear that it will have an impact on a force's ability to monitor terrorist activity.

Irrespective of what information is or isn't held, the public entrust the Police Service to make appropriate decisions with regard to their safety and protection and the only way of reducing risk is to be cautious with what is placed into the public domain.

The cumulative effect of terrorists gathering information from various sources would be even more impactful when linked to other information gathered from various sources about terrorism. The more information disclosed over time will give a more detailed account of the tactical infrastructure of not only a force area but also the country as a whole.

Any incident that results from such a disclosure would, by default, affect National Security.

Section 31 – Law Enforcement

Factors favouring confirming or denying that information is held

Confirmation that information exists relevant to this request would lead to a better informed public which may encourage individuals to provide intelligence in order to reduce such security breaches.

Factors against confirming nor denying that information is held

Confirmation or denial that information is held in this case would suggest Staffordshire Police take their responsibility to protect information and information systems from unauthorised access, destruction, etc., dismissively and inappropriately.

Balance Test

The points above highlight the merits of confirming or denying the requested information exists. The Police Service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. As part of that policing purpose, information is gathered which can be highly sensitive relating to high profile investigative activity. Weakening the mechanisms used to monitor any type of criminal activity, and specifically terrorist activity would place the security of the country at an increased level of danger.

In addition anything that places that confidence at risk, no matter how generic, would undermine any trust or confidence individuals have in the Police Service. Therefore, at this moment in time, it is our opinion that for these issues the balance test favours neither confirming nor denying that information is held.

Freedom of Information Request Appeals Procedure

1. Who Can Ask for a Review

Any person who has requested information from Staffordshire Police, which has been dealt with under the Freedom of Information Act, is entitled to complain and request an internal review, if they are dissatisfied with the response they received.

2. How to Request a Review



STAFFORDSHIRE
POLICE

Requests for review of a Freedom of Information request must be made in writing within two months of the date of receipt of this email, and should be addressed to:

foi@staffordshire.police.uk

Or by Post to:

Central Disclosure Unit
Staffordshire Police HQ
PO Box 3167
Stafford
ST16 9JZ

The reference number, date of the request and details of why the review is being requested must be included. Requests for review should be brought to the attention of the Central Disclosure Unit within two months of the Force's response to the original FOI request.

3. Review Procedure

Receipt of a request for review will be acknowledged in writing. The review will be conducted by another Decision Maker who is independent from the original Decision Maker. The Central Disclosure Unit will set a target date for a response. The response will be made as soon as is practicable with the intention to complete the review within 20 working days. In more complex cases the review may take up to 40 working days.

The independent Decision Maker will conduct a review of the handling of the request for information and of decisions taken, including decisions taken about where the public interest lies in respect of exempt information where applicable. The review enables a re-evaluation of the case, taking into account the matters raised by the complaint.

4. Conclusion of the Appeal

On completion of the review the Independent Decision maker will reply to the complainant with the result of the review. If the complainant is still dissatisfied following the review they should contact the Information Commissioner to make an appeal. The Information Commissioner can be contacted via the following details:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ICO Website for complaints link: <https://ico.org.uk/make-a-complaint/foi-and-eir-complaints/foi-and-eir-complaints/>

Freedom of Information
Central Disclosure Unit